UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/082,385	02/25/2002	Kuldip Singh Pabla	5181-94200	4546

7590 04/07/2006

Robert C. Kowert
Conley, Rose, & Tayon, P.C.
P.O. Box 398
Austin, TX 78767

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/082,385	PABLA ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/03/06, 03/27/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 56-65 have been amended.

2. Claims 1-65 are pending.

Response to Arguments

3. Applicant's arguments filed 27 December 2005 have been fully considered but they are not persuasive.

4. Referring to the rejection of claim 1, the Applicant contends that the prior art (Huitema et al. nor Klonowski) disclose or suggest a second peer determining if a session with the first peer is to be established in response to the message indicating the first peer is requesting a session with the second peer. The Examiner respectfully disagrees and assets that Klonowski discloses a secure network data communication technique by using an advanced peer-to-peer networking (APPN) system. The advanced peer-to-peer networking system provides communication such as message routing, which allows session establishment and routing services between the first peer and the second peer. When an APPN node (first peer) wishes to establish a session with another node (second peer), the first peer initiates a request. (See Figure 6 and Column 5, lines 56-65. This determination is made through the use of sharing keys between the two peers to the network node hosting the second peer. The network node initiates a request communication by transmitting it into the network. In response, the second peer receives a message indicating that the first peer is requesting a session with the second peer. (See Column 6, lines 6-12) Therefore, if it is determined that a

secured session is to be established, then a session key may be generated and sent to the first peer in a message (See Column 6, lines 13-28)

5. The rejection of claims 1-65 are maintained in view of the reasons above and in view of the reasons below.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huitema et al. (Pub No. 2003/0056093) in view of Klonowski (US Patent No. 5,479,514).

Referring to the rejection of claims 1,15,25,29,33,45, and 56, Huitema et al. discloses a method and network comprising:

a first peer sending a message to a second peer on a peer-to-peer network, wherein the message indicates that the first peer is requesting a session with the second peer; (See Page 7, Section 0054 and Figure 3)

the first peer sending a first public key to the second peer; (See Page 7, Section 0054)

the second peer receiving the first message; (See Page 7, Section 0055 and Figure 4)

the second peer receiving the first public key; (See Page 7, Section 0055)

the second peer determining if a session with the first peer is to be established in response to the message indicating the first peer is requesting a session with the second peer; (See Page 7, Section 0056 and Figure 5)

However, Huitema et al. fails to explicitly disclose a session key. Klonowski discloses a peer-to-peer network comprising:

if it is determined that a session with the first peer is to be established: the second peer generating a first session key from the first public key; (See Column 6, lines 13-16)

the second peer sending a message including the first session key to the first peer indicating that the second peer accepts the request for the session; (See Column 6, lines 16-27)

and the first peer receiving the message including the first session key; and the first peer and the second peer using the first session key to encrypt and decrypt data exchanged between the first peer and the second peer to provide secure exchange of the data between the first peer and the second peer on the peer-to-peer network (See Column 6, lines 28-36)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Huitema et al.'s peer-to-peer group method by using Klonowski encrypted communication. Klonowski provides a secure method for data to be exchanged within a peer-to-peer communication by incorporating a session key. (See Klonowski, Column 2, lines 23-35)

Referring to claims 2,16,26,30,34,46, and 57, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein the data comprises one or more chat messages (See Huitema et al., Page 6, Sections 0050-0051)

Referring to claims 3,17,35,47, and 58, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein the data comprises one or more files (See Huitema et al., Page 5, Section 0042)

Referring to claims 4 and 36, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein if it is determined that a session with the first peer is not to be established, the second peer sending a message to the first peer indicating that the second peer rejects the request for the session (See Huitema et al., Page 8, Section 0066)

Referring to claims 5,18,37,48, and 59, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein if it is determined that a session with the first peer is to be established:

encrypting the message including the first session key on the second peer using the first public key prior to the sending the message including the first session key; (See Klonowski, Column 6, lines 55-67, Column 7, lines 1-8)

and decrypting the message including the first session key on the first peer using a private key corresponding to the first public key after the receiving the message including the first session key (See Klonowski, Column 7, lines 10-31)

Referring to claims 6,19, and 60, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein ending the session between the first peer and the second peer; (See Klonowski, Column 6, lines 55-67, Column 7, lines 1-8)

establishing a new session between the first peer and the second peer subsequent to ending the session; (See Klonowski, Column 7, lines 9-30)

generating a second session key for the new session, wherein the second session key is different than the first session key; (See Klonowski, Column 7, lines 36-46)

and the first peer and the second peer using the second session key to encrypt and decrypt data exchanged between the first peer and the second peer in the new session to provide secure exchange of the data between the first peer and the second peer on the peer-to-peer network (See Klonowski, Column 7, lines 52-59)

Referring to claims 7 and 31, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein generating a second session key for the new session comprises:

the first peer generating a second public key; (See Huitema et al., Page 6, Section 0052)

the first peer sending the second public key to the second peer on the peer-to-peer network; (See Huitema et al., Page 7, Section 0054)

the second peer receiving the second public key; (See Huitema et al., Page 7, Section 0055)

and the second peer generating the second session key from the second public key (See Klonowski, Column 7, lines 52-59)

Referring to claim 8, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein the second peer sending the second session key to the first peer and the first peer receiving the second session key (See Klonowski, Column 7, lines 52-59)

Referring to claims 9 and 39, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein the session is a chat session (See Klonowski, Column 3, lines 54-60)

Referring to claims 10,11,21,40,41,51,52, and 62, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein a third peer sending a third public key to the first peer; (See Klonowski, Column 6, lines 55-67, Column 7, lines 1-4)

the first peer generating a third session key from the third public key wherein only the first peer and the third peer possess the third session key; (See Klonowski, Column 7, lines 4-14)

the third peer sending a fourth public key to the second peer; (See Klonowski, Column 7, lines 14-18)

and the second peer generating a fourth session key from the fourth public key, wherein only the second peer and the third peer possess the fourth session key (See Klonowski, Column 7, lines 18-30)

Referring to claims 12,22,42,53, and 63, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein a third peer on the peer-to-peer network joining the session (See Klonowski, Column 3, lines 56-60)

providing the first session key to the third peer; (See Klonowski, Column 3, lines 60-64)

wherein the third peer is configured to encrypt messages to be send to the first peer and to the second peer using the first session peer using the first session key, and wherein the third peer is further configured to decrypt encrypted messages received from the first peer and from the second peer using the first session key (See Klonowski, Column 3, lines 65-67)

Referring to claims 13,23,27,43,54, and 64, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein the first public key and an associated private key are generated using the RSA (Rivest-Shamir-Adleman) algorithm (See Huitema et al., Page 5, Section 0038)

Referring to claims 14,24,28,32,44,55, and 65, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein the first peer and the second peer are configured to operate in accordance with a peer-to-peer platform in the peer-to-peer network, (See Huitema et al., Page 4, Sections 0031-0032)

wherein the peer-to-peer platform includes one or more protocols configured for use in communications among peers participating in the peer-to-peer network, (See Huitema et al., Page 4, Section 0034, Page 5, Section 0039)

and wherein the peer-to-peer platform furthers includes one or more policies that define rules and conventions for the peer participating in the peer-to-peer network, wherein the one or more protocols include a peer group discovery protocol configured for use by a peer in identifying a particular network region the peer is attached to and for discovering other peers attached to the particular network region (See Huitema et al., Page 7, Sections 0046 and 0053)

Referring to claims 20,50, and 61, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein the first peer and the second peer are participants in a chat session on the peer-to-peer network (See Klonowski, Column 3, lines 56-66)

Referring to claims 38 and 49, (Huitema et al. as modified by Klonowski) discloses the claimed limitation wherein ending the session between the first peer and the second peer; (See Klonowski, Column 6, lines 55-67, Column 7, lines 1-8)

establishing a new session between the first peer and the second peer subsequent to ending the session; (See Klonowski, Column 7, lines 9-30)

generating a second session key for the new session, wherein the second session key is different than the first session key; (See Klonowski, Column 7, lines 36-46)

the first peer and the second peer using the second session key to encrypt and decrypt data exchanged between the first peer and the second peer in the new session to provide secure exchange of the data between the first peer and the second peer on the peer-to-peer network (See Klonowski, Column 7, lines 52-59)

wherein generating a second session key for the first peer comprises:

generating a second public key; (See Huitema et al., Page 6, Section 0052)

sending the second public key to the second peer on the peer-to-peer network; (See Huitema et al., Page 7, Section 0054)

receiving the second public key; (See Huitema et al., Page 7, Section 0055)

generating the second session key from the second public key (See Klonowski, Column 7, lines 52-59)

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-

272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
March 24, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER